PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-328033
(43)Date of publication of application : 30.11.1999

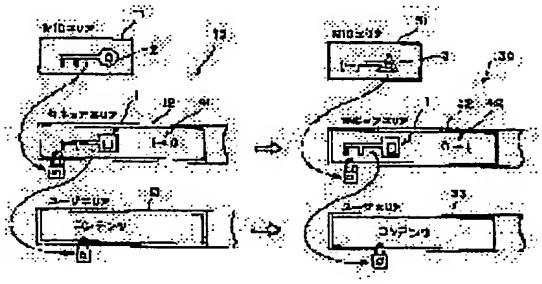
(51)Int.Cl. G06F 12/14
G06F 17/60
G09C 1/00

(21)Application number : 10-138663
(22)Date of filing : 20.05.1998

(71)Applicant : FUJITSU LTD
(72)Inventor : UCHIUMI KENICHI
HIRANO HIDEYUKI
KOTANI MASATAKE

(54) LICENSE TRANSFER DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To copy and deliver contents while protecting a person having a right to the use of the contents in a license transfer system which transfers the right to the use of contents.
SOLUTION: Contents are enciphered with a key 1, and this key 1 and information on use right 41 are enciphered with a key 2 consisting of a medium ID which specifies a storage medium 10 where they are stored. At the time of transferring the right to the use of the contents, contents enciphered by the key 1 are transferred to a storage medium 30 of a transfer destination as they are, and the key 1 and use right information 41 are deciphered by the medium ID of the storage medium of the transfer source and are enciphered by the medium ID of the storage medium of the transfer destination and are stored in the storage medium 30 of the transfer destination.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－328033

(43)公開日　平成11年(1999)11月30日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ａ
	17/60		Ｇ０９Ｃ	1/00	６６０Ｄ
Ｇ０９Ｃ	1/00	６６０	Ｇ０６Ｆ	15/21	Ｚ

審査請求　未請求　請求項の数７　ＯＬ　（全 13 頁）

(21)出願番号　特願平10－138663

(22)出願日　平成10年(1998)５月20日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　内海　研一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　平野　秀幸
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

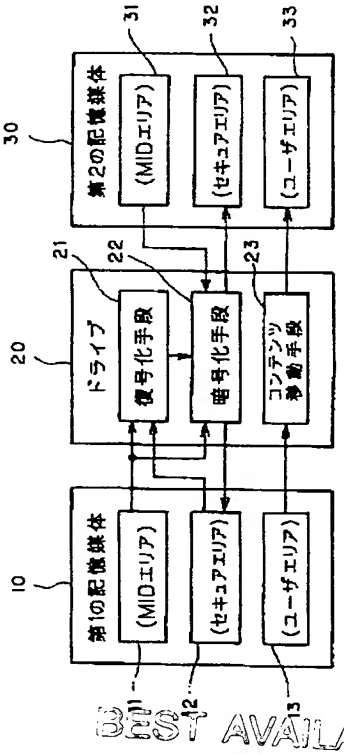
(74)代理人　弁理士　山田　正紀

(54)【発明の名称】　ライセンス委譲装置

(57)【要約】

【課題】本発明は、コンテンツの使用権を委譲するライセンス委譲システムに関し、そのコンテンツに関し権利を有する者の保護を図りつつ、そのコンテンツの複製や頒布等を行なう。

【解決手段】鍵１でコンテンツを暗号化し、その鍵１および使用権情報４１を、それらが格納された記憶媒体１０を特定するメディアＩＤからなる鍵２で暗号化しておき、そのコンテンツの使用権を委譲するにあたり、コンテンツは鍵１で暗号化された状態のまま、委譲先の記憶媒体３０に移し、鍵１および使用権情報４１を移転前の記憶媒体１０のメディアＩＤで復号化し、さらに委譲先の記憶媒体３０のメディアＩＤで暗号化して、委譲先の記憶媒体３０に格納する。



1

【特許請求の範囲】

【請求項１】　所定の鍵により暗号化されたコンテンツと、自分を特定する第１のメディアＩＤと、前記鍵と該コンテンツの使用権を表す第１の使用権情報との双方が一緒あるいは別々に前記第１のメディアＩＤで暗号化されてなる第１の暗号化セキュア情報とが格納された第１の記憶媒体と、自分を特定する第２のメディアＩＤが格納された第２の記憶媒体とをアクセスして前記第１の記憶媒体に格納されたコンテンツの使用権を前記第１の記憶媒体から前記第２の記憶媒体に委譲するライセンス委譲装置において、

前記コンテンツの使用権の委譲にあたり前記第１の記憶媒体に格納された第１の暗号化セキュア情報を前記第１のメディアＩＤを用いて復号化することにより前記鍵と前記第１の使用権情報とを得る復号化手段、および前記復号化手段による復号化により得られた鍵と、前記復号化手段による復号化により得られた第１の使用権情報があらわす第１の使用権が譲渡あるいは分与された第２の使用権をあらわす第２の使用権情報との双方を一緒にあるいは別々に前記第２のメディアＩＤで暗号化することにより第２の暗号化セキュア情報を生成して前記第２の記憶媒体に格納させる暗号化手段を備えたことを特徴とするライセンス委譲装置。

【請求項２】　前記暗号化手段が、さらに、前記第１の使用権から前記第２の使用権を差し引いた後の第３の使用権をあらわす第３の使用権情報を、あるいは前記鍵と該第３の使用権情報との双方を、前記第１のメディアＩＤで暗号化して前記第１の記憶媒体に書き戻すことにより、該第１の記憶媒体に、前記第１の暗号化セキュア情報に代えて、前記鍵と前記第３の使用権情報との双方が該第１のメディアＩＤで暗号化されてなる第３の暗号化メディア情報を格納させるものであることを特徴とする請求項１記載のライセンス委譲装置。

【請求項３】　前記第１の記憶媒体が持つ前記コンテンツの使用権全体を前記第２の記憶媒体に委譲する場合に、前記暗号化手段が、前記復号化手段による復号化により得られた鍵と、前記第１の使用権の全てを受け継いだ第２の使用権をあらわす第２の使用権情報とが暗号化されてなる第２の暗号化セキュア情報を生成して前記第２の記憶媒体に格納させるとともに、前記第１の記憶媒体に格納されている前記第１の暗号化セキュア情報を構成する前記鍵を破壊させるものであることを特徴とする請求項１記載のライセンス委譲装置。

【請求項４】　コンテンツの使用権委譲前において、前記第１の記憶媒体が、暗号化された、使用権を委譲しようとするコンテンツが格納されたものであって、

コンテンツの使用権の委譲にあたり、前記第１の記憶媒体に格納された、委譲対象の暗号化されたコンテンツを読み出して、暗号化された状態のまま、前記第２の記憶媒体に格納するコンテンツ移動手段を備えたことを特徴

2

とする請求項１記載のライセンス委譲装置。

【請求項５】　前記第１の使用権情報および前記第２の使用権情報が使用権が存在することをあらわすものであり、前記第３の使用権情報が使用権が存在しないことをあらわすものであることを特徴とする請求項１記載のライセンス委譲装置。

【請求項６】　前記第１の使用権情報が、第１の使用可能回数あるいは使用可能時間をあらわすものであり、前記第２の使用権情報が、該第１の使用可能回数あるいは使用可能時間以内の第２の使用可能回数あるいは使用可能時間をあらわすものであり、前記第３の使用権情報が、該第１の使用可能回数あるいは使用可能時間から該第２の使用可能回数あるいは使用可能時間を差し引いた後の第３の使用可能回数あるいは使用可能時間をあらわすものであることを特徴とする請求項１記載のライセンス委譲装置。

【請求項７】　前記第１の記憶媒体および前記第２の記憶媒体をそれぞれ駆動する第１のドライブおよび第２のドライブを備えるとともに、該第１のドライブおよび該第２のドライブが、前記第１の記憶媒体および前記第２の記憶媒体それぞれをアクセスする、それぞれ第１のファームウェアおよび第２のファームウェアを備えたものであり、

前記復号化手段および前記暗号化手段が、前記第１のファームウェアと前記第２のファームウェアとの複合体としてのファームウェア内に構成されたものであって、

前記第１のファームウェアのみが前記第１のドライブにより駆動される前記第１の記憶媒体をアクセスする権原を有するとともに、前記第２のファームウェアのみが前記第２のドライブにより駆動される第２の記憶媒体をアクセスする権原を有するものであることを特徴とする請求項１記載のライセンス委譲装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンテンツの使用権を第１の記憶媒体から第２の記憶媒体に委譲するライセンス委譲装置に関する。

【０００２】

【従来の技術】近年、如何にして著作権の保護の実効を図るかが問題となってきている。例えば本のような有形物の場合、頒布すること自体は複製を伴なわず、本を転売すればその本は購入者の手もとに渡り販売者のもとには本は存在しなくなり、したがって著作権の保護は比較的簡単であるが、ディジタル情報化された著作物の場合、例えばそのディジタル化された著作物をネットワークを介して送信すると自分側と相手側との双方に同じ著作物が発生し、頒布すること自体が複製を伴う結果となり、通常、このようなディジタル情報化された著作物に対する著作権の実効的な保護は極めて難しいとされている。

【０００３】
【発明が解決しようとする課題】本発明は、上記事情に鑑み、ディジタル化された文書、映画、プログラム等のコンテンツの使用権を、そのコンテンツに関し権利を有する者の保護を図りつつ委譲することのできるライセンス委譲装置を提供することを目的とする。
【０００４】
【課題を解決するための手段】上記目的を達成する本発明のライセンス委譲装置は、所定の鍵により暗号化されたコンテンツと、自分を特定する第１のメディアＩＤと、上記鍵とそのコンテンツの使用権を表す第１の使用情報との双方が一緒あるいは別々に第１のメディアＩＤで暗号化されてなる第１の暗号化セキュア情報とが格納された第１の記憶媒体と、自分を特定する第２のメディアＩＤが格納された第２の記憶媒体とをアクセスして第１の記憶媒体に格納されたコンテンツの使用権を第１の記憶媒体から第２の記憶媒体に委譲するライセンス委譲装置において、コンテンツの使用権の委譲にあたり第１の記憶媒体に格納された第１の暗号化セキュア情報を第１のメディアＩＤを用いて復号化することにより上記鍵と上記第１の使用権情報とを得る復号化手段、および上記復号化手段による復号化により得られた鍵と、および上記復号化手段による復号化により得られた第１の使用権情報があらわす第１の使用権が譲渡あるいは分与された第２の使用権をあらわす第２の使用権情報との双方を一緒にあるいは別々に上記第２のメディアＩＤで暗号化することにより第２の暗号化セキュア情報を生成して第２の記憶媒体に格納させる暗号化手段を備えたことを特徴とする。
【０００５】ここで、上記本発明のライセンス委譲装置において、上記暗号化手段は、さらに、上記第１の使用権から上記第２の使用権を差し引いた後の第３の使用権をあらわす第３の使用権情報を、あるいは鍵と上記第３の使用権情報との双方を、上記第１のメディアＩＤで暗号化して第１の記憶媒体に書き戻すことにより、第１の記憶媒体に、上記記第１の暗号化セキュア情報に代えて、上記鍵と上記第３の使用権情報との双方が第１のメディアＩＤで暗号化されてなる第３の暗号化メディア情報を格納させるものであってもよく、あるいは、第１の記憶媒体が持つ上記コンテンツの使用権全体を第２の記憶媒体に委譲する場合に、上記暗号化手段は、上記復号化手段による復号化により得られた鍵と、上記第１の使用権の全てを受け継いだ第２の使用権をあらわす第２の使用権情報とが暗号化されてなる第２の暗号化セキュア情報を生成して第２の記憶媒体に格納させるとともに、第１の記憶媒体に格納されている第１の暗号化セキュア情報を構成する鍵を破壊させるものであってもよい。
【０００６】尚、上記の、「鍵と、……第１の使用権情報との双方が一緒にあるいは別々に第１のメディアＩＤで暗号化されてなる第１の暗号化セキュア情報」は、鍵を第１のメディアＩＤで暗号化し、これとは別に第１の使用権情報を第１のメディア情報で暗号化し、それらの暗号化された鍵と暗号化された第１の使用権情報とを合わせたものを第１の暗号化セキュア情報と称してもよく、あるいは、鍵と第１の使用権情報との双方を連ねたものを第１のメディア情報で暗号化し、その暗号化された情報を第１の暗号化セキュア情報と称してもよいことを意味している。
【０００７】また、上記の、「鍵と、……第２の使用権情報の双方を一緒にあるいは別々に……第２のメディアＩＤで暗号化することにより第２の暗号化セキュア情報を生成して……」や「鍵と、……第３の使用権情報との双方が第１のメディアＩＤで暗号化されてなる第３の暗号化セキュア情報」も同様である。さらに、上記の、「第３の使用権情報を、あるいは……鍵と……第３の使用権情報との双方を、……第１のメディアＩＤで暗号化して……」は、鍵と、第１の使用権情報あるいは第２の使用権情報を別々に暗号化するシステムにおいては、第３の使用権情報のみを暗号化すればよく、鍵と第１（あるいは第２）の使用権情報を連ねたものを暗号化するシステムにおいては、鍵と第３の使用権情報との双方を連ねたものを暗号化することを意味している。
【０００８】本発明のライセンス委譲装置は、例えばＭＯ（光磁気ディスク）やハードディスクには、それぞれに固有のＩＤ（メディアＩＤと称する）が付されている点に着目し、完成されたものである。所定の鍵で暗号化されたコンテンツを流通させることによりその暗号化されたコンテンツ自体はその鍵を用いて復号化しない限り使用不可能である。そこで、その暗号化されたコンテンツを復号化するための鍵と、使用権情報（例えばそのコンテンツの使用が許可されているか否かという情報など）との双方を、その記憶媒体独自のメディアＩＤで暗号化しておく。こうすることにより、その暗号化されたコンテンツは、そのコンテンツがもともと格納された記憶媒体を離れてそれ自体が頒布されても使用不能であり、鍵もそのまま頒布したのでは頒布を受けた先ではメディアＩＤが異なるため鍵を復号化することはできず、したがって使用権のない者による無断使用が防止できる。
【０００９】このようなシステムにおいて、自分（第１の記憶媒体）の使用権を委譲先（第２の記憶媒体）に譲り渡すには、自分（第１の記憶媒体）のメディアＩＤで鍵および自分の使用権情報を復号化し、自分の使用権の範囲（例えば使用可能な残存回数）の中で使用権を分与し（あるいはその使用権全体であってもよい）、鍵と、その分与されたあるいは全体としての使用権情報を、委譲先（第２の記憶媒体）のメディアＩＤ（第２のメディアＩＤ）で暗号化してその委譲先（第２の記憶媒体）に格納させる。自分（第１の記憶媒体）には、残りの使用権（使用権が存在しないという使用権を含む）を自分

（第１の記憶媒体）のメディアＩＤ（第１のメディアＩＤ）で暗号化して自分（第１の記憶媒体）に書き戻す。あるいは使用権の全部を委譲する場合は、自分（第１の記憶媒体）では、残りの使用権（この場合は使用権が存在しないという使用権）を暗号化して書き戻す代わりに、自分（第１の記憶媒体）に暗号化された形式で格納されている鍵を破壊してしまってもよい。こうすることにより、そのコンテンツに関し権利を有する者の権利を犯すことなく使用権の譲渡が可能となる。

【００１０】ここで、上記本発明のライセンス委譲装置は、コンテンツの使用権委譲前において、第１の記憶媒体が、暗号化された、使用権を委譲しようとするコンテンツが格納されたものであって、コンテンツの使用権の委譲にあたり、第１の記憶媒体に格納された、委譲対象の暗号化されたコンテンツを読み出して、暗号化された状態のまま、第２の記憶媒体に格納するコンテンツ移動手段を備えることが好ましい。

【００１１】コンテンツ自体は暗号化された状態のまま頒布されるので、いつ頒布してもよく、例えば既に頒布されているときは鍵と使用権のみを渡せばよいが、例えば上記のコンテンツ移動手段を備えて、コンテンツの使用権の委譲にあたりそのコンテンツを第１の記憶媒体から第２の記憶媒体に移動（複製）してもよい。また、上記本発明のライセンス委譲装置において、上記第１の使用権情報および上記第２の使用権情報が使用権が存在することをあらわすものであり、上記第３の使用権情報が使用権が存在しないことをあらわすものであってもよく、あるいは、上記第１の使用権情報が、第１の使用可能回数あるいは使用可能時間をあらわすものであり、上記第２の使用権情報が、その第１の使用可能回数あるいは使用可能時間以内の第２の使用可能回数あるいは使用可能時間をあらわすものであり、上記第３の使用権情報が、第１の使用可能回数あるいは使用可能時間から第２の使用可能回数あるいは使用可能時間を差し引いた後の第３の使用可能回数あるいは使用可能時間をあらわすものであってもよい。

【００１２】このほか、例えば使用権を有する人を特定するＩＤを使用権情報としてもよく、使用権情報は、使用権の有無や範囲をあらわす情報であればどのような情報であってもよい。また、上記本発明のライセンス委譲装置において、第１の記憶媒体および第２の記憶媒体をそれぞれ駆動する第１のドライブおよび第２のドライブを備えるとともに、第１のドライブおよび第２のドライブが、第１の記憶媒体および第２の記憶媒体それぞれをアクセスする、それぞれ第１のファームウェアおよび第２のファームウェアを備えたものであり、上記復号化手段および上記暗号化手段が、上記第１のファームウェアと上記第２のファームウェアとの複合体としてのファームウェア内に構成されたものであって、上記第１のファームウェアのみが第１のドライブにより駆動される第１の記憶媒体をアクセスする権原を有するとともに、上記第２のファームウェアのみが第２のドライブにより駆動される第２の記憶媒体をアクセスする権原を有するものであることが好ましい。

【００１３】ここで、「第１のファームウェアのみが……第１の記憶媒体をアクセスする権原を有する」、「第２のファームウェアのみが……第２の記憶媒体をアクセスする権原を有する」は、例えばアプリケーションプログラム等からは、それら第１のファームウェアや第２のファームウェアを介在させずに直接には第１の記憶媒体や第２の記憶媒体をアクセスすることはできないように構成されていることを意味し、このような構成を備えると以下のような場合を含め、コンテンツに関する正当な権利を有する者の権利が一層確実に保護されることになる。

【００１４】すなわち、仮に、ファームウェアを介在させずにアプリケーションプログラムから直接に記憶媒体をアクセスすることができるシステムの場合、第１の記憶媒体から第２の記憶媒体に使用権を委譲する前にアプリケーションプログラムで第１の記憶媒体を直接にアクセスして上述した第１の暗号化セキュア情報を読み出して第３の記憶媒体に格納しておく。このような前準備を行なった上で使用権を第１の記憶媒体から第２の記憶媒体に委譲する。その委譲が終了した後、再びアプリケーションプログラムで第１の記憶媒体を直接にアクセスして第３の記憶媒体にあらかじめ復製しておいた委譲前の第１の暗号化セキュア情報を第１の記憶媒体に書き戻す。この場合、第１の記憶媒体は使用権を委譲する前の状態に戻り、かつ第２の記憶媒体にも使用権が発生し、正当な権利者の権利が犯される結果をもたらす。

【００１５】そこで、上記のようにファームウェアのみからアクセスを可能とすることにより、上記のような不正の発生を未然に防止することができ、正当な権利者の権利をより一層確実に保護することができる。

【００１６】

【発明の実施の形態】以下、本発明の実施形態について説明する。ここでは解り易さのため、概念的な実施形態について先ず説明し、次いで具体的な実施形態について説明する。図１は、本発明のライセンス委譲装置の一実施形態を示す構成図、図２は、その説明のための模式図である。

【００１７】図１には、第１の記憶媒体１０、ドライブ２０、および第２の記憶媒体３０が示されている。第１の記憶媒体１０および第２の記憶媒体３０は、いずれも、その記憶媒体の種類を問うものではないが、その記憶媒体を特定するメディアＩＤを有することが必要である。このメディアＩＤは、同種の記憶媒体を互いに確実に識別するものである必要はなく、例えば同一のメディアＩＤを持つ２つの記憶媒体が出会うことがほとんど期待できない程度にその記憶媒体にユニークなものであれ

ばよい。

【００１８】ドライブ２０は、本実施形態では、第１の記憶媒体１０を駆動する第１のドライブ、例えば第１の記憶媒体１０がMO（光磁気ディスク）の場合の光磁気ディスクドライブ装置と、第２の記憶媒体３０を駆動する第２のドライブ、例えば第２の記憶媒体３０がハードディスクの場合そのハードディスクを駆動するハードディスクドライブ装置との複合体として観念される。

【００１９】また、第１のドライブには、そのマイクロコンピュータとそのマイクロコンピュータで動作するソフトウェアとの組合せからなる、第１のドライブにより駆動される第１の記憶媒体をアクセスするための第１のファームウェアが搭載されており、これと同様に、第２のドライブにも、マイクロコンピュータとそのマイクロコンピュータで動作するソフトウェアとの組合せからなる、その第２のドライブにより駆動される第１の記憶媒体をアクセスするための第２のファームウェアが搭載されている。ここでは、第１のファームウェアと第２のファームウェアとの複合体としてのファームウェアがドライブ２０に搭載されているものと観念する。

【００２０】第１の記憶媒体１０および第２の記憶媒体２０は、それぞれ、自分自身のメディアＩＤを記憶しておくＭＩＤエリア１１，３１、使用権情報やその他コンテンツの属性に関する情報が格納されるセキュアエリア１２，３２、およびコンテンツ自身が格納されるユーザエリア１３，３３を有する。ここでは、第１の記憶媒体１０が持っているコンテンツの使用権を第２の記憶媒体３０に委譲しようとしており、したがってここでは、第１の記憶媒体１０のＭＩＤエリア１１，セキュアエリア１２，およびユーザエリア１３には、それぞれ、その第１の記憶媒体１０のメディアＩＤ、使用権情報やその他の属性、およびコンテンツが実際に格納されているものとする。

【００２１】一方、第２の記憶媒体３０のＭＩＤエリア３１には、その第２の記憶媒体３０のメディア３０のメディアＩＤが格納されているが、セキュアエリア３２、およびユーザエリア３３はあらかじめ領域として用意されていてもよく、あるいは、コンテンツの使用権の委譲にあたってそれらの領域が生成されるものであってもよい。

【００２２】以下において説明する復号化手段２１，暗号化手段２２，およびコンテンツ移動手段２３は、ドライブ２０内に搭載されたファームウェア内に構築されており、アプリケーションプログラムは、そのファームウェアを起動することはできるが、そのファームウェアの動作の内部に入り込んでそのファームウェアの動作を制御したり、あるいはそのファームウェアを介在させずに第１の記憶媒体や第２の記憶媒体を直接にアクセスすることはできないように構成されている。

【００２３】つまり、ＭＩＤエリア１１，３１は、ファームウェアによるリードが許可されライトが禁止されているエリアであり、アプリケーションは、ファームウェアを介在させた場合を含めて原則としてＭＩＤエリア１１，３１へのアクセスが禁止されている。また、セキュアエリア１２，３２とユーザエリア１３，３３はファームエリアによるリード・ライトが許可されているエリアであり、アプリケーションは、本実施形態では、ファームエリアを介在させた場合にのみセキュアエリア１２，３２とユーザエリア１３，３３にアクセスすることができ、直接リード・ライトを行うことはできない。但し、ユーザエリア１３，３３については、アプリケーションによる直接的なアクセスが許可されたエリアであってもよい。

【００２４】尚、ＭＩＤエリア１１，３１については、セキュアエリア１２，３２およびユーザエリア１３，３３とは独立に物理的に書き換え不可能な不揮発性の記憶媒体上に設けられていることが望ましい。但し、本実施形態ではＭＩＤエリアはセキュアエリアおよびユーザエリアとともに第１の記憶媒体および第２の記憶媒体上に設けられている。

【００２５】ここで、図２に示すように、第１の記憶媒体１０のユーザエリア１３に格納されたコンテンツは、鍵１で暗号化された形式で格納されており、その鍵１は、使用権情報４１とともに、ＭＩＤエリア１１に格納された、この第１の記憶媒体１０のメディアＩＤからなる鍵２で暗号化された形式で、セキュアエリア１２に格納されている。ここで、図２には、セキュアエリア１２に格納された使用権情報４１として、‘１→０’が示されているが、‘１’はそのコンテンツの使用権が存在することを意味し、‘０’はそのコンテンツの使用権が無いことを意味し、‘１→０’は、使用権の委譲前は‘１’であって、使用権委譲の際に‘０’に書き換えられることを意味している。また、図２において、セキュアエリア１２およびユーザエリア１３は、右にさらに延びるように描かれているが、これは、１つの記憶媒体（ここでは第１の記憶媒体１０）のユーザエリアに複数のコンテンツが格納され、それら複数のコンテンツそれぞれについて鍵や使用権情報等がセキュアエリア１２に格納される場合があることを意味している。

【００２６】ここで鍵１と使用権情報４１を鍵２で暗号化するにあたっては、この図２では、鍵１と使用権情報４１とを合わせた情報が鍵２で暗号化されているように描かれてれているが、そうであってもよく、あるいは、鍵１が鍵２で暗号化され、それとは別に、使用権情報４１が鍵２で暗号化されていてもよい。いずれの場合であっても、鍵２で暗号化された鍵１と、鍵２で暗号化された使用権情報との双方を合わせたものを、ここでは暗号化セキュア情報（本発明にいう第１の暗号化セキュア情報）と称する。

【００２７】コンテンツの使用権の委譲にあたり、図１

に示すドライブ２０の復号化手段２１により、第１の記憶媒体１０のＭＩＤエリア１１に記憶された、第１の記憶媒体１０のメディアＩＤ（本発明にいう第１のメディアＩＤ）からなる鍵２で、セキュアエリア１２に格納された第１の暗号化セキュア情報が復号化され、その暗号化により平文の鍵１と使用権情報４１（ここでは、使用権が存在することを表わす‘１’）が取り出される。そこで、今度は、図１に示すドライブ２０の暗号化手段２２により、その復号化により平文に戻された鍵１と使用権情報４１（使用権が存在することをあらわす‘１’）が今度は、第２の記憶媒体３０のＭＩＤエリア３１に格納されたメディアＩＤ（本発明にいう第２のメディアＩＤ）からなる鍵３で暗号化されて第３の暗号化セキュア情報が生成され、第２の記憶媒体３０のセキュアエリア３２に格納される。図２における第２の記憶媒体３０のセキュアエリア３２に描かれた使用権情報４２が‘０→１’となっているのは、使用権の委譲を受ける前は使用権が存在せず‘０’であって、使用権の委譲を受けることにより使用権が存在することをあらわす‘１’に書き換えられたことを意味する。

【００２８】また、第１の記憶媒体１０には、復号化された使用権情報４１が、使用権が存在しないことをあらわす‘０’に書き換えられ、復号化された鍵１と、使用権が存在しないことをあらわす使用権情報が、第１の記憶媒体１０のメディアＩＤからなる鍵２で暗号化されて、新たな暗号化セキュア情報（本発明にいう第３のセキュア情報）が生成され、それまで第１の記憶媒体１０のセキュアエリア１２に格納されていた第１の暗号化セキュア情報に代えて、その新たに生成された第３のセキュア情報がそのセキュアエリア１２に格納される。

【００２９】あるいは、第１の記憶媒体１０にはそのコンテンツの使用権が存在しなくなったのであるから鍵１は不要であり、第３のセキュア情報を生成して第１の記憶媒体１０のセキュアエリア１２に格納することに代え、そのセキュアエリア１２に暗号化された形式で格納されている鍵１を破壊してしまってもよい。また、第１の記憶媒体１０のユーザエリア１３に格納されている、鍵１で暗号化されたコンテンツは、図１に示すドライブ２０のコンテンツ移動手段２３により、第１の記憶媒体１０から読み出され、鍵１により暗号化された状態のまま、第２の記憶媒体３３のユーザエリア３３に格納される。

【００３０】以上により、それまで第１の記憶媒体１０が所有していた、コンテンツの使用権が、第２の記憶媒体２０に委譲される。それ以降、第２の記憶媒体２０を駆動する第２のドライブでは、アプリケーションプログラムからの、このコンテンツの読出し要求があると、その第２のドライブに搭載された第２のファームウェアは、第２の記憶媒体３０をアクセスし、その第２の記憶媒体３０のＭＩＤエリア３１に格納された、その第２の記憶媒体３０のメディアＩＤからなる鍵３で、セキュアエリア３２に格納された暗号化セキュア情報を復号化し、使用権が存在することを確認し、鍵１により、ユーザエリア３３に格納された、暗号化されたコンテンツを復号化し、その復号化されたコンテンツをアプリケーションプログラムに戻す。

【００３１】一方、その使用権を委譲した後は、第１の記憶媒体１０を駆動する第１のドライブでは、仮に、アプリケーションプログラムからの、その使用権を委譲したコンテンツの読み出し要求があった場合、その第１のドライブに搭載された第１のファームウェアは、第１の記憶媒体１０をアクセスし、その第１の記憶媒体のＭＩＤエリアに格納された、その第１の記憶媒体３０のメディアＩＤからなる鍵２で、そのセキュアエリア１２に格納された暗号化セキュア情報を復号化し、使用権の存在を確認したところ使用権が存在しないことを認識し、あるいは、上述の、鍵１を破壊するシステムの場合は、鍵１が破壊されていること、あるいはそのコンテンツを復号化できないことを認識し、アプリケーションプログラムに対し、そのコンテンツは読み出し不能である旨通知する。このようにして、コンテンツの使用権を、そのコンテンツに関し権利を有する者の権利を犯すことなく、有効に委譲することができる。

【００３２】ここで、上記実施形態では、簡単のため、使用権情報は、使用権が存在することをあらわす‘１’と使用権が存在しないことをあらわす‘０’との二値情報であるとして説明したが、使用可能回数を使用権情報として用いてもよい。例えば委譲前の第１の記憶媒体１０の使用権情報が使用可能回数１０回をあらわす‘１０’であったものとし、その使用可能回数の一部、例えば使用可能回数３回分のみを第２の記憶媒体３０に委譲してもよい。この場合、第２の記憶媒体３０の使用権情報は使用可能回数３回をあらわす‘３’となり、第１の記憶媒体１０には、使用権情報として、使用可能回数７回をあらわす‘７’が書き戻される。第１の記憶媒体１０あるいは第２の記憶媒体３０でそのコンテンツが使用されると、その使用のたびに、第１のドライブに搭載された第１のファームウェアあるいは第２のドライブに搭載された第１のファームウェアにより、その第１の記憶媒体１０あるいは第２の記憶媒体３０の使用可能回数が１ずつ減算される。

【００３３】ここで、第２の記憶媒体３０に委譲した３回分の使用権を使い切ってしまったとき、第１の記憶媒体１０に未だ使用権が残っていればその使用権の一部もしくは全部を上記と同一の手順で再度第２の記憶媒体に委譲することもできる。ただしその場合は、暗号化されたコンテンツ自体は既に第２の記憶媒体３０に移っているため、そのコンテンツ自体を第２の記憶媒体３０に移す必要はなく、そのコンテンツの使用権のみを第２の記憶媒体３０に移せばよい。

【００３４】尚、図２に示す例では、鍵１と使用権情報との双方を１つの情報と見なして、その情報を鍵２で暗号化することにより第１の記憶媒体１０用の暗号化セキュア情報を生成し、鍵１と使用権情報との双方を１つの情報とみなしてその情報を鍵３で暗号化することにより第２の記憶媒体３０用の暗号化セキュア情報を生成しているが、鍵１と使用権情報は、別々に暗号化してもよい。その場合、使用権の委譲にあたって鍵１は既に暗号化された形式で第１の記憶媒体１０に格納されているため、新たな使用権情報のみを暗号化して第１の記憶媒体１０に書き戻せばよい。また、使用可能回数を複数回に分けて委譲する場合、２回目以降の委譲の際は、第２の記憶媒体３０には鍵１が鍵３で暗号化された形式で既に格納されているため、委譲を受けた使用可能回数をあらわす使用権情報のみを鍵３で暗号化してセキュアエリア３２に書き込めばよい。

【００３５】また、鍵１と使用権情報のほか、例えばそのコンテンツの名称、そのコンテンツの最終アクセス日時等そのコンテンツの使用権情報以外の属性も一緒にセキュアエリアに格納してもよく、その場合に、それらの属性が暗号化する必要がないものである場合は平文のまま格納してもよく、あるいはそれらの属性が暗号化する必要がないものであっても、鍵１や使用権情報と一緒に暗号化してもよい。

【００３６】さらに、上記では使用権情報として、使用権の有無と、使用回数を取り挙げて説明したが、そのほかにも、使用可能時間を使用権情報としてもよく、アクセスが許諾された人をあらわすＩＤを使用権情報としてもよく、使用権の有無、あるいは使用可能範囲をあらわす種々の情報を使用権情報として使用することができる。

【００３７】図３は、本発明のライセンス委譲装置の一実施形態が搭載されたコンピュータシステムの一例を示す外観斜視図、図４は、そのコンピュータシステムの構成を示すブロック図である。このコンピュータシステム５０は、外観上は、図３に示すように、ＣＰＵやメモリ等が内蔵された本体部５１、表示画面５２ａ上に画像を表示する画像表示装置５２、このコンピュータシステム５０に対し各種の指示を行なうための操作子であるキーボード５３、および画像表示装置５２の表示画面５２ａ上の位置を指定するための操作子であるマウス５４により構成されている。また本体部５１には、ＭＯ（光磁気ディスク）１００が装填、取出し自在に装填されるＭＯ装填口５１ａが示されている。

【００３８】また、このコンピュータシステム５０は、内部構成上は、図４に示すように、各種のプログラムが実行されるＣＰＵ５５、実行されるプログラムやデータの一時的な格納領域として使用されるメモリ５６、キーボード５３との間でデータの受け渡しを行なうキーボードインターフェース５７、マウス５４の操作に伴うデータを伝えるマウスインターフェース５８、画像表示装置５２に表示用のデータを伝える表示インターフェース５９、図３に示すＭＯ装填口５１から装填されたＭＯ１００を駆動するＭＯドライブ６０、および内蔵されたハードディスク６２を駆動するハードディスクドライブ６１が備えられており、それらは、図４に示すように、バス６３で互いに接続されている。

【００３９】ここでは、図３，図４に示すコンピュータシステム５０内において、ＭＯ１００に格納されたコンテンツの使用権をハードディスク６２に委譲する場合を説明するが、使用権の単純な移動、あるいは、使用可能回数が設定されている場合において、その使用可能回数以内の一部の使用可能回数を初回に委譲する場合については、図１，図２を参照して既に説明済であるため、以下では、初回に委譲した使用可能回数を使い果たし、所定の使用可能回数を再度委譲する場合について説明する。また、図１，図２を参照した説明は、本発明の理解のために概念的な説明を行なったが、ここではより詳細な説明を行なう。

【００４０】図５は、ＭＯ１００に格納されたコンテンツの使用権をハードディスク６２に委譲する手順を示す図である。この図５には、アプリケーション６４とドライブ２０が示されている。アプリケーション６４は、ＣＰＵ５５で実行される、コンピュータシステム５０の操作者により直接に操作が可能なプログラムであって、ここでは、ＭＯ１００内のコンテンツの使用権をハードディスク６２に委譲することを指示するプログラムをあらわしている。また、ドライブ２０は、ここでは、図４に示すＭＯドライブ６０とハードディスクドライブ６１との複合体である。ＭＯ１００に格納されたコンテンツの使用権をハードディスク６２に委譲する手順を以下に説明するが、ここではＭＯ１００に、委譲しようとしているコンテンツを残り１０回使用することができる使用権が残っており、そのうちの３回の使用権をハードディスク６２に委譲するものとして説明する。

【００４１】ここでは簡単のため、委譲され得るコンテンツは１つのみ存在するものとし、コンテンツと称するときは、その委譲される（あるいはその委譲によりハードウェア６２に使用権が移った）コンテンツを意味するものとする。

（１）先ず、アプリケーション６４からドライブ２０に向けて、コンテンツの委譲元がＭＯ１００であり、コンテンツの委譲先がハードディスク６２であることを、ドライブ２０に向けて指定する（図５（Ａ））。

【００４２】（２）するとドライブ２０は、ＭＯ１００およびハードディスク６２をアクセスするための準備を行ない、ドライブ２０は、それらの準備が整った段階で、アプリケーション６４に対し準備が整ったことを報告する（図５（Ｂ））。

（３）すると、アプリケーション６４では、ドライブ２

０がアプリケーションに送る情報を隠蔽するためのパスワードをドライブ２０（ＭＯドライブ６０とハードディスクドライブ６１との双方）に送るとともに、ＭＯ１００のセキュアエリア（図１，図２参照）に格納されている使用権情報（ここでは、上述の前提どおり、使用可能回数をあらわす情報を使用権情報としており、ＭＯ１００には、現在１０回使用可能であることをあらわす使用権情報‘１０’が格納されているものとする）を読み出す命令をドライブ２０に向けて発行する（図５（Ｃ））。

【００４３】（４）すると、ドライブ２０を構成するＭＯドライブ６０（図４参照）内では、以下の処理が実行される。ここで、ＭＯドライブ６０内にもＣＰＵが搭載されており、さらに、装填されたＭＯ１００をアクセスするためのマイクロプログラムが搭載されており、それらＭＯドライブ６０のハードウェアとソフトウェアとを合せたファームウェアがＭＯドライブ６０における処理を実行することになる。

【００４４】（４－１）ＭＯ１００のＭＩＤエリア（図１，図２のＭＩＤエリア１１参照）からＭＯ１００のメディアＩＤを読み出す。

（４－２）ＭＯ１００のセキュアエリア（図１，図２のセキュアエリア１２参照）から、メディアＩＤで暗号化された使用権情報を読み出す。

（４－３）その読み出した使用権情報をメディアＩＤで復号化する。

【００４５】（４－４）上述（３）のステップにおいてアプリケーション６４から送られてきたパスワードで、復号化された使用権情報をエンコードする。

（４－５）そのエンコードされた情報をアプリケーション６４に伝える（図５（Ｄ））。

（５）すると、アプリケーション６４は、以下の処理を実行する。

【００４６】（５－１）ＭＯドライブ６０から送られてきた使用権情報をパスワードでデコードする。

（５－２）そのデコードされた使用権情報があらわす使用可能回数がこれ以上使用できないことをあらわす‘０’でないことを確認する（ここでは、説明の前提として使用可能回数１０回をあらわす‘１０’が設定されており、‘０’ではない）。

【００４７】（５－３）今度は、ドライブ２０に向けて、使用権の委譲先であるハードディスク６２の、使用権情報を読み出す命令を発行する（図５（Ｅ））。尚、前述したように、ここでは説明の前提として、ハードディスク６２には、前回、コンテンツを何回か使用することのできる使用権が設定され、その使用可能回数が‘０’になった場合を想定している。

【００４８】（６）すると、ハードディスク６２を駆動するハードディスクドライブ６１では以下の処理が実行される。ハードディスクドライブ６１にもＣＰＵやマイクロプログラムが備えられており、ハードディスクドライブ６１における処理も、ＭＯドライブ６０における処理と同様、それらハードウェアとソフトウェアとの複合体としてのファームウェアにより実行される。

【００４９】（６－１）ハードディスク６２のＭＩＤエリア（図１，図２のＭＩＤエリア３１参照）からハードディスク６２のメディアＩＤを読み出す。

（６－２）ハードディスク６２のセキュアエリア（図１，図２のセキュアエリア３２参照）から、ハードディスク６２のメディアＩＤで暗号化された使用権情報を読み出す。

【００５０】（６－３）その読み出した使用権情報を、ハードディスク６２のメディアＩＤで復号化する。

（６－４）上述の（３）のステップにおいてアプリケーション６４から送られてきたパスワードで、その復号化された使用権情報をエンコードする。（６－５）そのエンコードされた使用権情報をアプリケーション６４に伝える（図５（Ｆ））。

【００５１】（７）すると、アプリケーション６４は、以下の処理を実行する。

（７－１）ハードディスクドライブ６１から送られてきた使用権情報をパスワードでデコードする。

（７－２）そのデコードされた使用権情報が使用可能回数‘０’をあらわしていることを確認する。

【００５２】もし使用可能回数が‘０’でなく、まだ使用可能であることをあらわしているときは、本実施形態では、まだ使用可能である旨表示画面５２ａ（図３参照）に表示してオペレータにその旨通知し、この段階で処理を中断する。ここでは説明の前提として使用可能回数は‘０’であり、この場合、さらに以下の処理に進む。

【００５３】（７－３）ハードディスク６２に新たに設定される使用可能回数（ここでは説明の前提に基づいて３回）をあらわす情報（新回数情報と称する）をパスワードでエンコードしてドライブ２０（ＭＯドライブ６０とハードディスクドライブ６１との双方）に送る（図５（Ｇ））。

（８）ＭＯドライブ６０では、この新回数情報を受けて以下の処理が実行される。

【００５４】（８－１）ＭＯ１００のメディアＩＤを読み出す。

（８－２）ＭＯ１００のセキュアエリアに格納されている、ＭＯ１００のメディアＩＤで暗号化された状態の使用権情報を読み出す。

（８－３）その暗号化された使用権情報をＭＯ１００のメディアＩＤで復号化して使用可能回数‘１０’を取り出す。

【００５５】（８－４）アプリケーション６４から送られてきた、パスワードでエンコードされた新回数情報を、上述の（３）のステップで送られてきているパスワ

ードでデコードして使用可能回数‘３’を取り出す。
（８－５）ＭＯ１００にそれまで格納されていた使用可能回数‘１０’からハードディスク６２に譲渡しようとしている使用可能回数‘３’を差し引いて新たな使用可能回数‘７’を得る。
（８－６）その新たな使用可能回数‘７’をあらわす新たな使用権情報をＭＯ１００のメディアＩＤで暗号化する。
【００５６】（８－７）その暗号化された新たな使用権情報を、それまでＭＯ１００に格納されていた、使用可能回数‘１０’をあらわす使用権情報に上書きする。これにより、ＭＯ１００には使用可能回数‘７’が設定される。
（９）一方、ハードディスクドライブ６１では、上述の（７－３）のステップで送られてきた新回数情報を受けて、以下の処理が実行される。
【００５７】（９－１）ハードディスク６２のメディアＩＤを読み出す。
（９－２）アプリケーション６４から送られてきた、パスワードでエンコードされた新回数情報を、上述の（３）のステップで送られてきているパスワードでデコードして使用可能回数‘３’を取り出す。
（９－３）そのデコードにより取り出された使用可能回数‘３’をあらわす新たな使用権情報をハードディスク６２のメディアＩＤで暗号化する。
【００５８】（９－４）その暗号化された新たな使用権情報を、ハードディスク６２に格納されていた、使用可能回数‘０’をあらわす使用権情報に上書きする。これにより、ハードディスク６２には、使用可能回数‘３’が設定される。
（１０）以上の使用権委譲の処理が完了したことが、ドライブ２０からアプリケーション６４に通知される。
【００５９】以上のようにしてコンテンツの使用権の委譲（ここでは使用権の一部の委譲）が行なわれる。尚、図５を参照した以上の説明では、ＭＯ１００からハードディスク６２への、コンテンツ自体および暗号化されたコンテンツを復号化するための鍵の移動については言及されていないが、前述したように、ここでは、コンテンツの使用可能回数の再度の設定の場合を説明しており、したがってコンテンツ自体および、それを復号化するための鍵は初回の委譲時に既にハードディスク６２に渡されていることを前提としている。コンテンツ自体は、ＭＯ１００から初回の委譲時に暗号化された形式のままハードディスク６２に移動（複製）されており、また上記の説明は、鍵はそれぞれのメディアＩＤで使用権情報とは独立に暗号化されてそれぞれのセキュアエリアに格納されていることを前提としている。
【００６０】尚、図５を参照して説明した実施形態では、上述したように、アプリケーション６４とドライブ２０とが様々なコミュニケーションを行ないながらコンテンツの使用権の委譲の処理を進めているが、このようなコンテンツ委譲処理に代え、アプリケーション６４からは、使用権を委譲しようとしているコンテンツ、そのコンテンツの使用権の委譲元（ここではＭＯ１００）、委譲先（ここではハードディスク６２）、および委譲しようとしている、使用権の回数を指定し、その後はドライブ２０（ここではＭＯドライブ６０とハードディスクドライブ６１との双方）に処理を任せ、アプリケーション６４とは独立にドライブ２０において上記の委譲処理を実行し、委譲処理が終了した段階、および何らかの不都合により委譲処理が正常に行なわれなかった（例えばＭＯ１００に委譲を指定された使用可能回数未満の使用可能回数しか残っていなかった、あるいはハードディスク６２に前回に委譲を受けた使用可能回数がまだ‘０’になっていなかった、など）ときのみ、アプリケーション６４に報告するように構成してもよい。
【００６１】また、上記の委譲処理６０は、上記の説明ではＭＯドライブ６０とハードディスクドライブ６１とで分担して実行しているが、それらＭＯドライブとハードディスクドライブ６１とのうちの一方はアクセス専用とし、上記の委譲処理は、専らもう一方の側で行なうように構成してもよい。図６は、本発明のライセンス委譲装置の一実施形態が組み込まれたコンピュータネットワークの一例を示す図、図７は、そのコンピュータネットワークを構成するあるコンピュータシステムから別のコンピュータシステムに対し、コンテンツの使用権を委譲する際の手順を示す図である。
【００６２】ここには、コンテンツ管理用のコンピュータシステム７０と、コンテンツを使用する側の２台のコンピュータシステム８０，９０が示されており、それら３台のコンピュータシステム７０，８０，９０は、通信回線２００を介して互いに接続されている。各コンピュータシステム７０，８０，９０は、それぞれが図３に示すコンピュータシステム５０と同様の構成を備えている。すなわち、各コンピュータシステム７０，８０，９０は、各本体部７１，８１，９１、各画像表示装置７２，８２，９２、各キーボード７３，８３，９３および各マウス７４，８４，９４を備えており、さらに各コンピュータシステム７０，８０，９０は、それぞれが図４に示す内部構成と同様の内部構成を備えている。詳細説明は省略する。
【００６３】ここでは、コンテンツ管理用のコンピュータシステム７０は、ある会社の本店に設置され、コンテンツを使用する側のコンピュータシステム８０，９０はその会社の各支店に設置されているものとする。以下では、説明の簡単のため、本店、および各支店に設置されたコンピュータシステム７０，８０，９０を、そのまま本店７０、支店８０、支店９０と称する。
【００６４】ここでは本店で、各種のコンテンツの全支店分のライセンスを購入し、その本店から各支店にライ

センスを分配し、かつ、その本店で全支店分のライセンスを管理しているものとする。すなわち、ここでは、同一のコンテンツであっても本店において必要な数の使用権を購入し、そのコンテンツを必要とする支店にその使用権を分配する。ここでいう同一のコンテンツについての必要な数の使用権は、そのコンテンツの使用回数を意味するものではなく、同一の本を複数冊（例えば３冊）購入するのと同様に同一のコンテンツの使用権を必要に応じた数だけ購入し、ここではその購入した数の使用権を意味している。本店では、各コンテンツについて、購入した使用権の数から支店に対し使用権を頒布した数の残りの数が管理されており、各支店では、同一のコンテンツについての複数の使用権は不要であって、各コンテンツについて自分の支店に使用権が存在するか否かのみを管理している。本店および各支店では多数のコンテンツの使用権情報が管理されており、ここではそれら多数のコンテンツの使用権情報の一覧を‘許諾情報’と称する。

【００６５】ここでは、本店７０から各支店８０，９０に対し、既に様々なコンテンツの使用権が委譲されており、さらに今回、本店７０からある支店（ここでは支店８０とする）に対しあるコンテンツの使用権を委譲するものとし（ここでは、使用権の新たな委譲を行なおうとしているコンテンツを‘新コンテンツ’と称する）、ここでは、その新コンテンツの使用権を支店８０に委譲する場面について説明する。ここでは、新コンテンツの使用権は、本店７０のハードディスクから支店８０のハードディスクに委譲されるものとする。

【００６６】（１）先ず本店７０から支店８０に向けて新コンテンツの使用権を委譲する旨連絡する（図７（Ａ））。

（２）すると支店８０ではその連絡を受けて、支店８０のハードディスクを準備状態にし、アクセスの準備が整うと本店７０に対し準備ができたことを報告する（図７（Ｂ））。

【００６７】（３）すると本店７０では、支店８０から送られてくる情報を隠蔽するためのパスワードを支店８０に送出し、さらに支店８０のハードディスクのセキュアエリアに格納されている許諾情報（複数のコンテンツそれぞれの使用権の有無をあらわす情報の一覧）を送るよう命令を発行する（図７（Ｃ））。

（４）支店８０では、この命令を受けて以下の処理を実行する。

【００６８】（４－１）支店８０のハードディスクのメディアＩＤを読み出す。

（４－２）支店８０のハードディスクのセキュアエリアから、そのハードディスクのメディアＩＤで暗号化された許諾情報を読み出す。

（４－３）その読み出した許諾情報を読み出したメディアＩＤで復号化する。

（４－４）上記の（３）のステップにおいて本店７０から送られてきたパスワードで、その復号化された許諾情報と、さらに支店８０のハードディスクのメディアＩＤをエンコードする。

【００６９】（４－５）そのエンコードされた許諾情報およびメディアＩＤを本店７０に送る（図７（Ｄ））。

（５）すると、本店７０では、以下の処理を実行する。

（５－１）支店８０から送られてきた許諾情報およびメディアＩＤをパスワードでデコードする。

【００７０】（５－２）そのデコードされた許諾情報を見て、これから支店８０に使用権を移そうとしている新コンテンツに関する使用権が支店８０に存在しないことを確認する。これは、同一の支店に対し同一のコンテンツの使用権を重複設定するのを避けるためである。

（５－３）本店７０のハードディスクのメディアＩＤを読み出す。

【００７１】（５－４）本店７０のハードディスクのセキュアエリアから、そのハードディスクのメディアＩＤで暗号化された許諾情報、および、同じくそのメディアＩＤで暗号化された、使用権を許諾しようとしているコンテンツを復号化するための鍵を読み出す。

（５－５）その読み出した許諾情報および鍵を、読み出したメディアＩＤで復号化する。

【００７２】（５－６）その復号化された許諾情報を参照して、支店８０に使用権をあらたに委譲しようとしているコンテンツ（新コンテンツ）に関する使用権に残りがあることを確認する。残りがないときは、その新コンテンツの使用を許諾することができない旨支店８０に伝えることになるが、ここでは、その新コンテンツの使用権が本店７０に残っているものとする。

【００７３】（５－７）上記の（５－１）のステップでデコードした、支店８０の許諾情報中の、新コンテンツの使用権をあらわす情報を‘使用権なし’から‘使用権有り’に書き換える。

（５－８）その書き換えた許諾情報、および鍵の双方をパスワードでエンコードする。

【００７４】（５－９）本店７０のハードディスクのユーザエリアから、暗号化された新コンテンツを読み出す。

（５－１０）そのエンコードされた許諾情報および鍵、および暗号化されたままの新コンテンツを支店８０に送る（図７（Ｅ））。

（５－１１）また、本店７０内において、上記の（５－５）のステップで復号化した本店７０の許諾情報中の、支店８０に今回使用権を許諾した新コンテンツに関する使用権の数に関する情報を１だけ減算することにより新たな許諾情報に更新する。

【００７５】（５－１２）そのようにして更新された新たな許諾情報を、本店７０のハードディスクのメディアＩＤで暗号化する。

（５－１３）その暗号化された新たな許諾情報を、本店７０のハードディスクのセキュアエリアに、そこにそれまで格納されていた更新前の許諾情報に代えて格納する。

【００７６】（６）支店８０では、上記の（５－１０）のステップで送られてきた、エンコードされた許諾情報および鍵、および暗号化された新コンテンツを受け取り、以下の処理を実行する。

（６－１）受け取った新コンテンツを、暗号化されたまま自分（支店８０）のハードディスクのユーザエリアに格納する。

【００７７】（６－２）受け取った許諾情報および鍵を、上述のステップ（３）で送られてきているパスワードでデコードする。

（６－３）自分（支店８０）のハードディスクのメディアＩＤを読み出す。

（６－４）パスワードでデコードされた許諾情報および鍵を、その読み出したメディアＩＤで暗号化する。

【００７８】（６－５）その暗号化された許諾情報および鍵を、自分（支店８０）のハードディスクのセキュアエリアに、それまで格納されていた許諾情報を書き換えるようにして格納する。以上により、その新コンテンツの使用権が本店７０から支店８０に委譲される。

【００７９】以上の各実施形態に示すように、本発明のライセンス委譲装置は、１台のコンピュータ等からなる１台の装置内においても、あるいは複数台のコンピュータ等を接続したネットワーク内においても実現可能である。

【００８０】

【発明の効果】以上説明したように、本発明によれば、コンテンツに関し権利を有する者の権利を犯すことなく、そのコンテンツを複製したり頒布したりすることができる。

【図面の簡単な説明】

【図１】本発明のライセンス委譲装置の一実施形態を示す構成図である。

【図２】図１に示すライセンス委譲装置の説明のための模式図である。

【図３】本発明のライセンス委譲装置の一実施形態が搭載されたコンピュータシステムの一例を示す外観斜視図である。

【図４】図３に外観を示すコンピュータシステムの構成を示すブロック図である。

【図５】ＭＯに格納されたコンテンツの使用権をハードディスクに委譲する手順を示す図である。

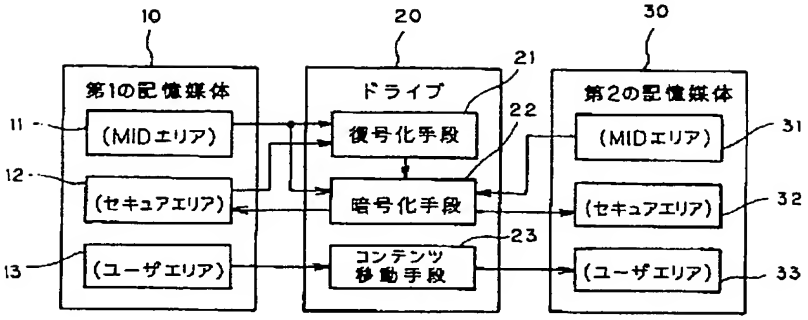
【図６】本発明のライセンス委譲装置の一実施形態が組み込まれたコンピュータネットワークの一例を示す図である。

【図７】図６に示すコンピュータネットワークを構成するコンピュータシステムから別のコンピュータシステムに対し、コンテンツの使用権を委譲する際の手順を示す図である。

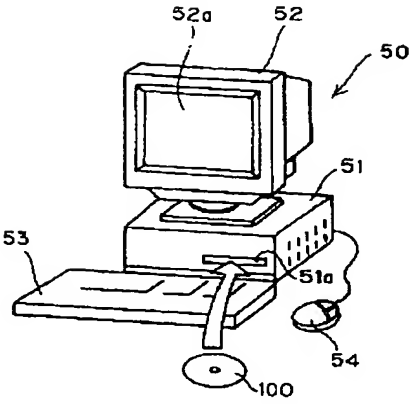
【符号の説明】

１０　第１の記憶媒体
１１　ＭＩＤエリア
１２　セキュアエリア
１３　ユーザエリア
２０　ドライブ
２１　復号化手段
２２　暗号化手段
２３　コンテンツ移動手段
３０　第２の記憶媒体
３１　ＭＩＤエリア
３２　セキュアエリア
３３　ユーザエリア
４１，４２　使用権情報
５０　コンピュータシステム
５１　本体部
５１ａ　ＭＯ装填口
５２　画像表示装置
５２ａ　表示画面
５３　キーボード
５４　マウス
５５　ＣＰＵ
５６　メモリ
５７　キーボードインターフェース
５８　マウスインターフェース
５９　表示インターフェース
６０　ＭＯドライブ
６１　ハードディスクドライブ
６２　ハードディスク
７０，８０，９０　コンピュータシステム
７１，８１，９１　本体部
７２，８２，９２　画像表示装置
７３，８３，９３　キーボード
７４，８４，９４　マウス
１００　ＭＯ（光磁気ディスック）
２００　通信回線

【図１】

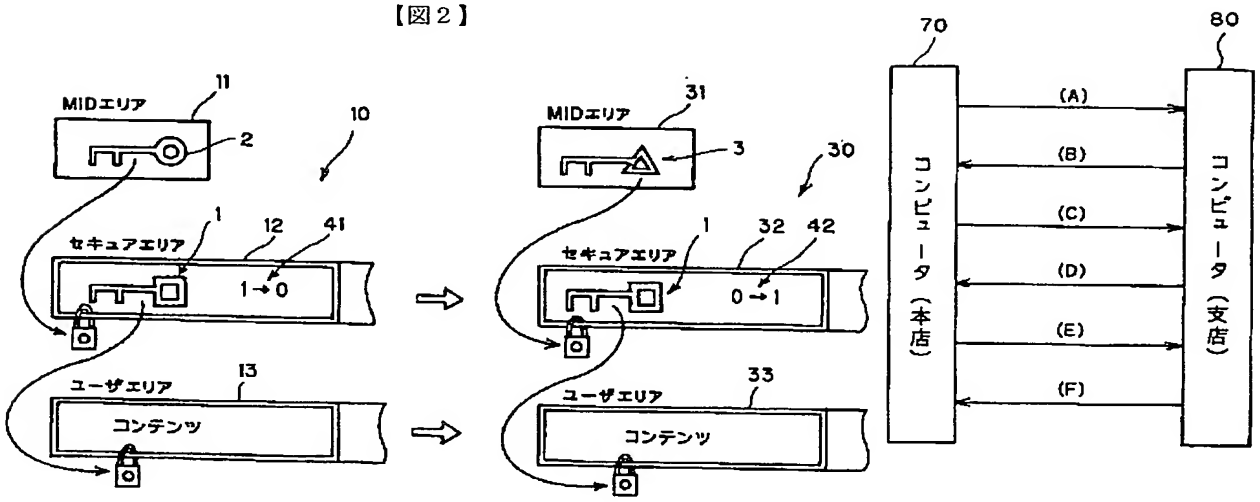


【図３】

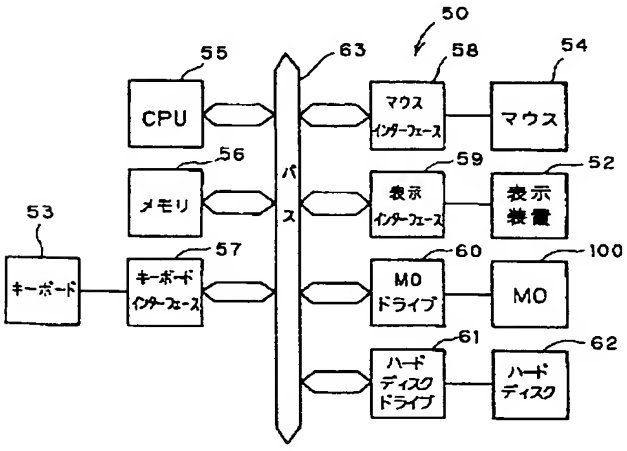


【図７】

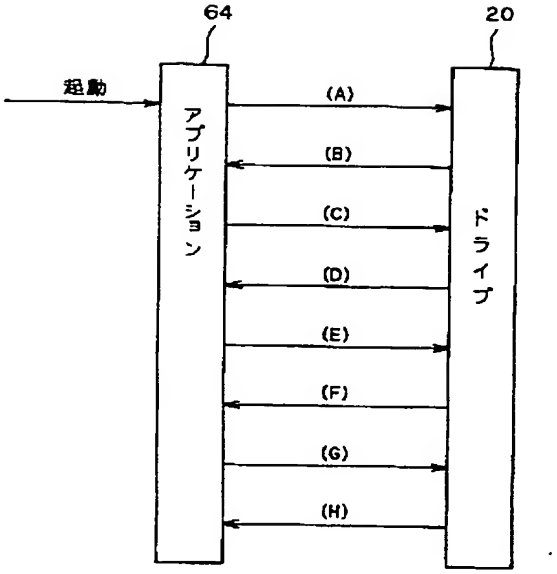
【図２】



【図４】



【図５】



【図６】